

Steven Jaewan Yang

2208 Hollowoak Dr. Hanover, Maryland 21076

Mobile: (443) 718-8303

Email: jyang127@terpmail.umd.edu

Portfolio Website: <https://sjymine.com> | LinkedIn: <https://www.linkedin.com/in/steven-yang-2691a3153/>

Work Experience:

Cyber Security Engineer - Contract

Careful Security

12100 Wilshire Blvd Suite 800 Los Angeles, CA

6/2022 - 10/2022

Duties, Accomplishments, and Related Skills:

Increased 20% to 80% SOC 2 compliance in the AWS cloud environment.

Implemented PCI DSS and CIS Benchmark Compliances on AWS cloud environments.

Integrated AWS Cloud Security services like Web Application Firewall, GuardDuty, CloudTrail, CloudWatch, Macie, S3 buckets, and Systems Manager with SIEMS like Wazuh.

Configured CloudTrail with Cloudwatch custom metric filters and created notification systems with SNS topics. Created custom network architecture on AWS Cloud using services such as S3, Auto-scaling groups, Load balancers, and Kinesis.

Tech Support Associate

Infosys Limited

One American Square Suite# 2200 Indianapolis, IN

12/2020 - 5/2022

Duties, Accomplishments, and Related Skills:

Analyzing data streams from the network and application using Splunk.

Review incident alerts and run vulnerability tests

Escalate to L2 Analyst with proper security analyst report

CA-PAM configuration with AD servers and its users and group policies. Mounted this PAM software onto VMware server clusters.

Configured Palo Alto firewalls so it provides high availability in on-premise data centers.

Assisted in creating internet access with Global Protect client for VPN access.

Education:

University of Maryland College Park – College Park, MD, United States

Bachelor of Science, Information Science – Cybersecurity

Relevant Coursework, Licenses, and Certifications:

Associate of ISC2 - CISSP | AWS Certified Security - Specialty | AWS Certified Solutions Architect -Associate | Purdue University

Enterprise Security | Purdue University Cybersecurity Foundations | CompTIA Network+ ce | ITIL Foundations

Projects:

Key logger Project - Python program that simulates reconnaissance and malware deployment through port ssh and default username and password. Using the tkinter module and .desktop file configuration, the innocent looking desktop icon can run python script (keylogger) once the image has been clicked.

Reference: <https://sjymine.com/loggingapp/>

Ransomware Project in AWS: By leveraging a typical developer user that has misconfigured IAM roles like "S3FullAccessrole", a ransomware attack is simulated and encrypted S3 buckets and its content. Explanation of RSA PKCS1_OAEP and AES OMAC1/CMAC encryption algorithm is also provided.

Reference: https://sjymine.com/ran_some_info/index.html

2DES Vulnerability Project - Python program that uses DES block cipher using Cipher Feedback Mode (CFB) that simulates the vulnerability of using 2DES by finding its intermediary data by encryption forward and decryption backwards to "meet in the middle".

Reference: https://sjymine.com/des_ofb/

Web Scraping Reddit Project - After web scraping CISSP subreddit, metadata that has been scraped is organized and filtered into a SQLite database. The database filters specific columns and finds commonly used phrases in subreddit posts. First query and create a new table when the post contains "%passed%" in title and comment column. Then extract 3 digit numbers that are listed before and after 'questions' or 'passed at' respectively. Then find the avg() using the built-in SQL command.

Reference: https://sjymine.com/web_scraper/index.html